10-02-00

A

JC926 U.S. PTO
09/29/00

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 042390.P9326

First Named Inventor or Application Identifier Manav Mishra

Express Mail Label No. EL580086885US

JC511 U.S. PTO
09/675694
09/29/00

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 18)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 4)

4. ____ Oath or Declaration/Power of Attorney (Total Pages ____)
   a. ___ Newly Executed (Original or Copy)
   b. ___ Copy from a Prior Application (37 CFR 1.63(d))
   (for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
   i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ____ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ____ Microfiche Computer Program (Appendix)

7. ____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
   a. ___ Computer Readable Copy
   b. ___ Paper Copy (identical to computer copy)
   c. ___ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. _____ Assignment Papers (cover sheet & documents(s))
9. _____ 37 CFR 3.73(b) Statement (where there is an assignee)
10. _____ English Translation Document (if applicable)
11. _____ a. Information Disclosure Statement (IDS)/PTO-1449
    _____ b. Copies of IDS Citations
12. _____ Preliminary Amendment
13. X Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. _____ a. Small Entity Statement(s)
    _____ b. Statement filed in prior application, Status still proper and desired
15. _____ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. X Other: Unsigned Declaration and Power of Attorney

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:
    ___ Continuation ____ Divisional ____ Continuation-in-part (CIP)
    of prior application No: _____

18. **Correspondence Address**
    _____ Customer Number or Bar Code Label _____ (Insert Customer No. or Attach Bar Code Label here)
    or
    X Correspondence Address Below

NAME Libby N. Ho Reg. No. 46,774

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025
(303) 740-1980 Telephone (303) 740-6962 Facsimile

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" Mailing Label No. EL580086885US to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Sept. 29, 2000
Date of Deposit

April Worley
Name of Person Mailing Correspondence

April Worley 9/29/00
Signature Date

PTO/SB/17(6/99)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL FOR FY 2000

TOTAL AMOUNT OF PAYMENT ($) 1092.00

Complete if Known:
Application No.
Filing Date Concurrently Herewith
First Named Inventor Manav Mishra
Group Art Unit Not Yet Assigned
Examiner Name Not Yet Assigned
Attorney Docket No. 042390.P9326

METHOD OF PAYMENT (check one)

1. [X] **The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:**

Deposit Account Number 02-2666
Deposit Account Name

[X] **Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17**

---

2. X **Payment Enclosed:**
X **Check**
____ **Money Order**
____ **Other**

FEE CALCULATION

1. **BASIC FILING FEE**

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility application filing fee	690.00
106	310	206	155	Design application filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional application filing fee	

SUBTOTAL (1) $690.00

2. **EXTRA CLAIM FEES**

			Extra Claims		Fee from below		Fee Paid
Total Claims	25	– 20** =	5	X	18.00	=	90.00
Independent Claims	7	– 3** =	4	X	78.00	=	312.00
Multiple Dependent						=	

**Or number previously paid, if greater; For Reissues, see below.

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
103	18	203	9	Claims in excess of 20	90.00
102	78	202	39	Independent claims in excess of 3	312.00
104	260	204	130	Multiple dependent claim, if not paid	0.00
109	78	209	39	**Reissue independent claims over original patent	0.00
110	18	210	9	**Reissue claims in excess of 20 and over original patent	0.00

SUBTOTAL (2) $ 402.00

FEE CALCULATION (continued)

Patent fees are subject to annual revisions. Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid.
See Forms PTO/SB/09-12

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,360	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive unavoidably abandoned application	
141	1,210	241	605	Petition to revive unintentionally abandoned application	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	690	246	345	For filing a submission after final rejection (see 37 CFR 1.129(a))	
149	690	249	345	For each additional invention to be examined (see 37 CFR 1.129(a))	
Other fee (specify)					
Other fee (specify)					

SUBTOTAL (3) $ 0.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name: Libby N. Ho

Signature _____ Date September 29, 2000

Reg. Number 46, 774 Deposit Account User ID _____ (complete if applicable)

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL580086885US

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, DC 20231.

Sept. 29, 2000
Date of Deposit

April Worley
Name of Person Mailing Correspondence

9/29/00

Do not use this space

Jc511 U.S. PTO
09/675694
09/29/00

Serial/Patent No.: _____ Filing/Issue Date: Concurrently Herewith
Client: Intel Corp.
Title: "Mechanism for Locking Client Requests to a Particular Server"
BSTZ File No.: 042390.P9326 Atty/Secty Initials: LNH/amw
Date Mailed: Sept. 29, 2000 Docket Due Date: —

The following has been received in the U.S. Patent & Trademark Office on the date stamped hereon:

- ☐ Amendment/Response (____ pgs.)
- ☐ Appeal Brief (____ pgs.) (in triplicate)
- ☒ Application - Utility (18 pgs, with cover and abstract)
- ☐ Application - Rule 1.53(b) Continuation (____ pgs.)
- ☐ Application - Rule 1.53(b) Divisional (____ pgs.)
- ☐ Application - Rule 1.53(b) CIP (____ pgs.)
- ☐ Application - Rule 1.53(d) CPA Transmittal (____ pgs.)
- ☐ Application - Design (____ pgs.)
- ☐ Application - PCT (____ pgs.)
- ☐ Application - Provisional (____ pgs.)
- ☐ Assignment and Cover Sheet
- ☒ Certificate of Mailing
- ☒ Declaration & POA (5 pgs.) unsigned
- ☐ Disclosure Docs & Orig & Copy of Inventor's Signed Later (____ pgs)
- ☒ Drawings: 4 # of sheets includes 4 figures
- ☒ Express Mail No. EL580086885US ☒ Check No. 795 Amt. 1092.-
- ☐ _____ Month(s) Extension of Time ☐ Check No. _____ Amt. _____
- ☐ Information Disclosure Statement & PTO-1449 (__ pgs.)
- ☐ Issue Fee Transmittal
- ☐ Notice of Appeal
- ☐ Petition for Extension of Time
- ☐ Petition for _____
- ☒ Postcard
- ☐ Power of Attorney (____ pgs.)
- ☐ Preliminary Amendment (____ pgs.)
- ☐ Reply Brief (____ pgs.)
- ☐ Response to Notice of Missing Parts
- ☐ Small Entity Declaration for Indep. Inventor/Small Business
- ☒ Transmittal Letter, in duplicate
- ☒ Fee Transmittal, in duplicate

☐ Other: _____

"Express Mail" mailing label number: EL580086885US
Date of Deposit: 9/29/00
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D. C. 20231

April Worley
(Typed or printed name of person mailing paper or fee)

April Worley
(Signature of person mailing paper or fee)

9/29/00
(Date signed)

Attorney Docket No.: 042390.P9326 Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

MECHANISM FOR LOCKING CLIENT REQUESTS TO A PARTICULAR SERVER

INVENTORS

MANAV MISHRA
SATYENDRA YADAV

Prepared by

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026
(303) 740-1980

Express Mail Label No. EL580086885US

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL580086885US
Date of Deposit: September 29, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D. C. 20231

April Worley
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

September 29, 2000

MECHANISM FOR LOCKING CLIENT REQUESTS TO A PARTICULAR SERVER

COPYRIGHT NOTICE

Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever.

FIELD OF THE INVENTION

This invention relates to the field of server load balancing, Internet quality of service, and security and more specifically, to a mechanism for locking client requests to a particular server.

BACKGROUND OF THE INVENTION

The demand for e-commerce brings a unique set of challenges to network infrastructures. For example, one server may be inadequate to provide the required capacity and scalability to serve the increasing size of e-commerce transactions. Server load balancing (SLB) was developed to overcome this problem, where a number of servers (server farm) act as a single server and a special device (dispatcher) dispatches requests to server in a manner that balances the load on all the servers in the serve farm. Some SLB schemes may dispatch requests to the server having the least load, and other SLB schemes may dispatch requests to any server such that the network is optimized, for example. For purposes of simplicity, the server selected by any given SLB scheme is referred to herein as the "best server".

In e-commerce transactions hosted on a website, however, SLB

introduces a new problem. When a customer sends information to a website that utilizes an SLB scheme, the information is sent to the best server computed by the dispatcher, Server A, and stored locally on that server. For example, a customer of Amazon.com® selects books and places them in the shopping cart, and then decides to visit other areas of the site before purchasing. When the customer returns to the shopping cart, effectively to access state information (the state of previously stored information), the SLB scheme again computes the best server, this time Server B, to direct the customer's request to. Since the distribution of requests amongst the servers in the server farm may have changed since the customer's last request, the best server on the subsequent request is different from the best server on the first request. Consequently, the customer's information does not exist on Server B, and the shopping cart may be empty when the customer returns to it.

One current solution to this problem is to globally maintain state information, such that the state information can be accessed by any server in the server farm. For example, state information can be maintained in a special state server, or even one of the servers in the server farm. One of the disadvantages to this, however, is the latency associated with memory accesses by the servers, as well as dispatcher latency associated with storing state information.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

FIG. 1 illustrates an exemplary server load balancing (SLB) environment in which preferred embodiments of the present invention are operable.

FIG. 2 illustrates elements in an exemplary environment.

FIG. 3 is a method of preferred embodiments of the invention.

FIG. 4 illustrates how quality of service can be applied in embodiments of the present invention.

Docket No.: 042390.P9326 : Express Mail Label: EL580086885US

DETAILED DESCRIPTION OF THE INVENTION

In one aspect of the invention, a method for directing requests from the same client in a single session to the same server in secure e-commerce transactions is described. In one exemplary use for this method, a user submits state information, hereinafter referred to as a client request, over the Internet to an e-commerce website, such as Amazon.com®, and the state information is stored on a system server. The e-commerce website comprises a dispatcher (a system for sending client requests to a server) and server farm (a pool of a plurality of servers for processing client requests). The client request is received by the dispatcher, and a unique session identifier (I.D.) is assigned to the client request. The dispatcher selects a server to send the client request to, and sends the client request to the selected server. The session I.D. is mapped to a server identifier associated with the selected server.

In preferred embodiments, when the client request is received by the dispatcher, the dispatcher establishes a secure connection, preferably SSL (Secure Sockets Layer), with the client. The dispatcher then uses a load balancing algorithm to determine the best server in the server farm to send the client request to. The unique session I.D. is then mapped to an SSL context, which identifies a previously existing SSL tunnel between the dispatcher and the selected server, such that subsequent requests having the same session I.D. can be directed to the same server via the SSL tunnel.

The present invention includes various operations, which will be described below. The operations of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the operations. Alternatively, the operations may be performed by a combination of hardware and software.

The present invention may be provided as a computer program product,

which may include a machine-readable medium having stored thereon instructions which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnet or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions. Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer (e.g., a server) to a requesting computer (e.g., a client) by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection). Accordingly, herein, a carrier wave shall be regarded as comprising a machine-readable medium.

Introduction

FIG. 1 illustrates an exemplary environment in which preferred embodiments of the present invention are operable. A user on a client system 100 logs into a server system 116 to conduct transactions, such as to browse the contents of a website, purchase goods from a website, or request information from a website. The server system 116 comprises a dispatcher 104 and a server farm 106 comprising a plurality of servers 108, 110, 112, 114. The dispatcher receives user requests to process transactions and selects one of the servers 108, 110, 112, 114 to send a given user request to. On a first session of a given user, the dispatcher 104 preferably selects a server 108, 110, 112, 114 from the server farm by using a load balancing algorithm to find the best server. Preferably, the dispatcher selects the same server that was selected for the user's first session on subsequent sessions for the same user if the request comprises secure information.

FIG. 3 outlines a method of the present invention starting at block 300. A first user request comprising a session I.D. is received at block 302. At block

304, it is determined if the transaction is a secure transaction. If it is, then at block 306, it is determined if the session I.D. exists in the mapping table. If the session I.D. does not exist in the mapping table, or if the transaction is not secure, then at block 310, a load-balancing algorithm is used to find the best server. Furthermore, the user request is sent to the best server at block 312. If the user request is a secure transaction, then at block 314, the mapping table is updated to include an entry for the session I.D. and the corresponding SSL context for the selected server.

If the transaction is secure and the session I.D. exists, then at block 308, the session I.D. is searched for in the mapping table, and the request is sent to the server corresponding to the session I.D. The method ends at block 316.

Secure Transactions

In preferred embodiments, the dispatcher distinguishes between secure and non-secure transactions. Secure transactions may be determined by the server system. For instance, secure transactions may be determined to comprise credit card transactions, a user's personal information, or user reviews. Non-secure transactions may be determined to comprise a user request for a book rating, for instance. As described herein, secure transactions refer to transactions in which information needs to be saved. Such information, such as personal data, and credit card information, is referred to as state information.

If a user request is determined to be a secure transaction, the dispatcher processes the request differently than if the request were a non-secure transaction. In preferred embodiments, the dispatcher 104 has previously existing SSL (Secure Sockets Layer) tunnels and corresponding SSL contexts 118, 120, 122 with the servers 108, 110, 112, 114 in the server farm 106 to handle secure transactions. An SSL tunnel is a designated channel of communication, and a corresponding SSL context comprises a source IP (Internet protocol) address, a destination IP address, and an encryption algorithm

that identifies a corresponding SSL tunnel.

Initial User Session Requests

When the user logs onto a website associated with a server system 116 to conduct a secure transaction, as shown in FIG. 2, the dispatcher 104 looks in a mapping table 204 to determine if the session I.D. has already been mapped to a specific server. If not, an SSL tunnel and corresponding SSL context 200 between the dispatcher 104 and the client 100 is created. The SSL context between the client 100 and the dispatcher 104 additionally comprises a session I.D. to uniquely identify the user's current login session. For example, a user logs onto Amazon.com®, places items in the shopping cart, submits the items for payment, and then decides to continue browsing the site.

The dispatcher 104 uses a load-balancing algorithm (by employing a load balancer, for instance), to find which one of the servers 108, 110, 112, 114 in the server farm 106 can best handle the current user request. As discussed, *supra*, the best server can be the server currently having the least load, or the server which can best alleviate network traffic, for instance. A load-balancing table 202 is updated accordingly.

Once a best server is determined, the user request is sent to the selected server 108. The dispatcher then maps the current session I.D. to the SSL context between the dispatcher 104 and the selected server 108 by adding an entry to a mapping table 204 for the session I.D. and the SSL context. The selected server receives the user's request, and stores corresponding information in its local memory for subsequent access.

Subsequent User Session Requests

When the user makes another request, (for example, the user has finished browsing the site and wishes to return to the shopping cart previously submitted), the dispatcher receives the subsequent request. Using the session I.D. from the

user request, the dispatcher 104 determines if the session I.D. exists in the mapping table 204. If the session I.D. exists in the mapping table 204, then the dispatcher sends the user's subsequent request to the server corresponding to the session I.D. as indicated by the mapping table 204. Since the previously submitted information is stored on this server, the user's information is quickly accessed on the server, and available to the user.

If the session I.D. does not exist in the mapping table 204, then processing proceeds as described for an initial user session request, *supra*.

Quality of Service

Where multiple requests are received on the same SSL tunnel between the dispatcher and a given server, a QoS (Quality of Service) Manager uses predetermined algorithms to aggregate multiple streams into a single stream. In reference to FIG. 4, when multiple clients, such as Client 1 404, and Client 2 402, are directed to the same server via an SSL tunnel, as determined by the load balancer 204, a QoS Manager 400 decides which client gets priority of the SSL tunnel. An exemplary algorithm used by the QoS Manager can be found in pending United States patent application entitled "Secure Communications Over Unsecure Links" by Manav Mishra, Raj Yavatkar, and Prakash Iver, filed on September 5, 2000, serial no. _____.

FIG. 4 further illustrates that when Client 1 404A, 406A submits a request to the dispatcher 104, Client 1 may submit a secure transaction 404B or a non-secure transaction 406B. If Client 1 submits a non-secure transaction, then a load balancer 204 determines which server in the server farm the client request is to be sent to via the current SSL connection 406B. If Client 1 submits a secure transaction, then a mapping table 204 is searched to determine if a session I.D. associated with Client 1 exists in the table. If it does, then the client request is sent to the server corresponding to the session I.D. in the mapping table 204. If the session I.D. does not exist, then a load balancer 410 uses a load balancing

table 202 to determine which server in the server farm to direct the client request to. Client 1 request is then sent to the selected server 408.

Where a second client, Client 2 402A, makes a client request and the load balancer 410 directs Client 2 request to the same server as Client 1, both requests 404B, 402B are sent to a QoS Manager 400 and, the QoS Manager decides which request to handle first. In the example of FIG. 4, Client 1's secure request 404B is a high-priority SSL request, and Client 2's secure request is a low-priority SSL request. The QoS Manager 400 then processes the requests according to their priorities, such that Client 1 404B receives a high-priority SSL connection with one of the servers in the server farm 408, and Client 2 402B receives a low-priority SSL connection with one of the servers in the server farm 412.

Non-Secure Transactions

In one embodiment, if a user request is determined to be a non-secure transaction, the dispatcher processes all user requests in the same way. In other words, the dispatcher uses a load balancing algorithm to find the best server, and forwards all requests to the best server determined at the time a request is received.

In other embodiments, non-secure (non-SSL) transactions can always be mapped to the same server using the scheme for secure transactions by using a cookie, or a block of data, as the session I.D. (rather than the SSL context in the case of a secure transaction). The cookie would be generated by the best server and returned to the client. When another client request is made from the same client, the cookie comprises information about the server that generated the cookie so that the request can be sent to the original server.

Conclusion

As described in embodiments of this invention above, the latency

associated with global accesses is alleviated, since information is locally stored at selected servers. Moreover, there is no loss of information since the same server is selected to process user requests.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

For example, while embodiments herein have been described to distinguish between secure and non-secure transactions, the invention can be implemented without making this distinction. In other words, regardless of the type of user request, the dispatcher may forward all user requests in the same session to the server for processing.

042390.P9326

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a first request comprising a session identifier (I.D.);

assigning a unique I.D. to the first request;

selecting one of a plurality of servers to process the first request;

assigning the unique I.D. to the selected server; and

sending the first request to the server.

2. A method as in claim 1, additionally comprising:

subsequently receiving a second request comprising the session I.D.;

selecting the server that the session I.D. is assigned to; and

sending the second request to the server.

3. A method as in claim 1, wherein said selecting one of a plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to the first request to.

4. A method comprising:

receiving a first request comprising a session identifier (I.D.);

selecting one of a plurality of servers to process the first request;

mapping the session I.D. to the selected server;

sending the first request to the selected server;

subsequently receiving a second request comprising the session I.D.;

determining that the second request comprises secure information;

selecting the server that the session I.D. is assigned to; and

sending the second request to the server.

5. A method as in claim 4, wherein the server is identified by an SSL (Secure Sockets Layer) context.

6. A method as in claim 4, wherein said selecting one of a plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to route the first request to.

7. A method as in claim 4, additionally comprising:

determining that the second request comprises non-secure information; and

using a load balancing algorithm to determine a server to route the second request to.

8. A method comprising:

receiving a first request comprising a session identifier (I.D.);

selecting one of a plurality of servers to process the first request, the server having a unique SSL (Secure Socket Layer) context, and the unique SSL context being associated with an SSL tunnel;

mapping the session I.D. to the selected SSL context;

sending the first request to the selected server;

subsequently receiving a second request comprising the session I.D.;

determining that the second request comprises secure information;

selecting the SSL context that the session I.D. is assigned to; and

sending the second request to the server via the SSL tunnel associated with the SSL context.

9. A method as in claim 8, wherein said selecting one of a plurality of servers to process the first request comprises using a load balancing algorithm to determine a server to route the first request to.

10. A method as in claim 8, additionally comprising:

determining that the second request comprises non-secure information; and

using a load balancing algorithm to determine a server to route the second request to.

11. A method comprising:

receiving a request comprising a session identifier (I.D.);

determining if the session I.D. is associated with an SSL (Secure Sockets Layer) context;

determining if the request is associated with a secure transaction;

if no session I.D. is associated with an SSL context, then selecting one of a plurality of servers to process the first request, the server having a unique SSL (Secure Socket Layer) context, and the unique SSL context being associated with an SSL tunnel; and

if the request is associated with a secure transaction, then:

mapping the session I.D. to the selected SSL context; and

sending the second request to the server via the SSL tunnel associated with the SSL context.

12. A method as in claim 11, wherein said selecting one of a plurality of servers to process the request comprises using a load balancing algorithm to determine a server to route the request to.

13. A method as in claim 11, wherein said determining if the request is associated with a secure transaction comprises determining if an SSL packet is associated with the request.

14. A method as in claim 11, wherein said determining if the session I.D. is associated with an SSL (Secure Sockets Layer) context comprises looking up the session I.D. in a mapping table to determine if the mapping table comprises an entry for the session I.D. and a corresponding SSL context.

15. A system comprising a dispatching processor unit to:

receive a first request comprising a unique session identifier (I.D.);

select a server from a plurality of servers to process the request;

assign the unique session I.D. to the selected server, and store the unique session I.D. and corresponding identifier for the selected server in a mapping table comprising entries of session I.D.s each having a corresponding server identifier;

send the first request to the selected server;

receive a second request comprising the unique session I.D.;

find the unique session I.D. in the mapping table; and

send the second request to the server corresponding to the unique session I.D. in the mapping table.

16. A system as in claim 15, wherein a preexisting SSL (Secure Sockets Layer) tunnel exists between the dispatching processor unit and the selected server, the SSL tunnel being identified by an SSL context, and the mapping table comprising entries of session I.D.s each having a corresponding SSL context.

17. A system as in claim 15, wherein the dispatching processing unit selects

one of a plurality of servers to process the request by using a load balancing algorithm to determine a server to route the request to.

18. A system as in claim 17, wherein the dispatching processing unit uses a load balancing algorithm to determine a server to route the request to by employing a load balancer.

19. A system comprising:

a dispatching processor unit to:

send client requests to a plurality of servers in a server farm;

receive a client request comprising a session identifier (I.D.);

determine if state information associated with the session I.D. already exists on one of a plurality of servers in the server farm;

send the client request to the server if the state information already exists on a server; and

employ a load balancer to determine one of the servers to send the client request to if the state information does not already exist on a server;

a load balancer in communication with the dispatching processor unit to determine one of a plurality of servers to send the client request to; and

a quality of service (QoS) manager in communication with the dispatching processor unit to decide which one of multiple client requests is processed if multiple client requests are sent to the same server.

20. A system as in claim 19, wherein the dispatching processor unit determines if state information associated with the session I.D. already exists on one of a plurality of servers in a server farm by searching a

mapping table comprising a session I.D. mapped to a server.

21. A system as in claim 20, wherein the session I.D. is mapped to a server by the session I.D. being associated with an SSL (Secure Sockets Layer) context, and the SSL context is associated with the server.

22. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive a first request comprising a session identifier (I.D.);

select one of a plurality of servers to process the first request;

map the session I.D. to the selected server;

send the first request to the selected server;

subsequently receive a second request comprising the session I.D.;

determine that the second request comprises secure information;

select the server that the session I.D. is assigned to; and

send the second request to the server.

23. A medium as in claim 22, wherein the server is identified by an SSL (Secure Sockets Layer) context.

24. A medium as in claim 22, wherein the processor selects one of a plurality of servers to process the first request by using a load balancing algorithm to determine a server to route the first request to.

25. A medium as in claim 22, the processor to additionally:

determine that the second request comprises non-secure information; and

usea load balancing algorithm to determine a server to route the second request to.

ABSTRACT OF THE INVENTION

In one aspect of the invention is a method for locking in all client requests having the same session I.D. to the same server to facilitate secure e-commerce transactions. A client's session I.D. is mapped to an SSL context between a dispatcher and a server such that all subsequent client requests having the same session I.D. are forwarded to the same server.

042390.P9326

006260 "6995960

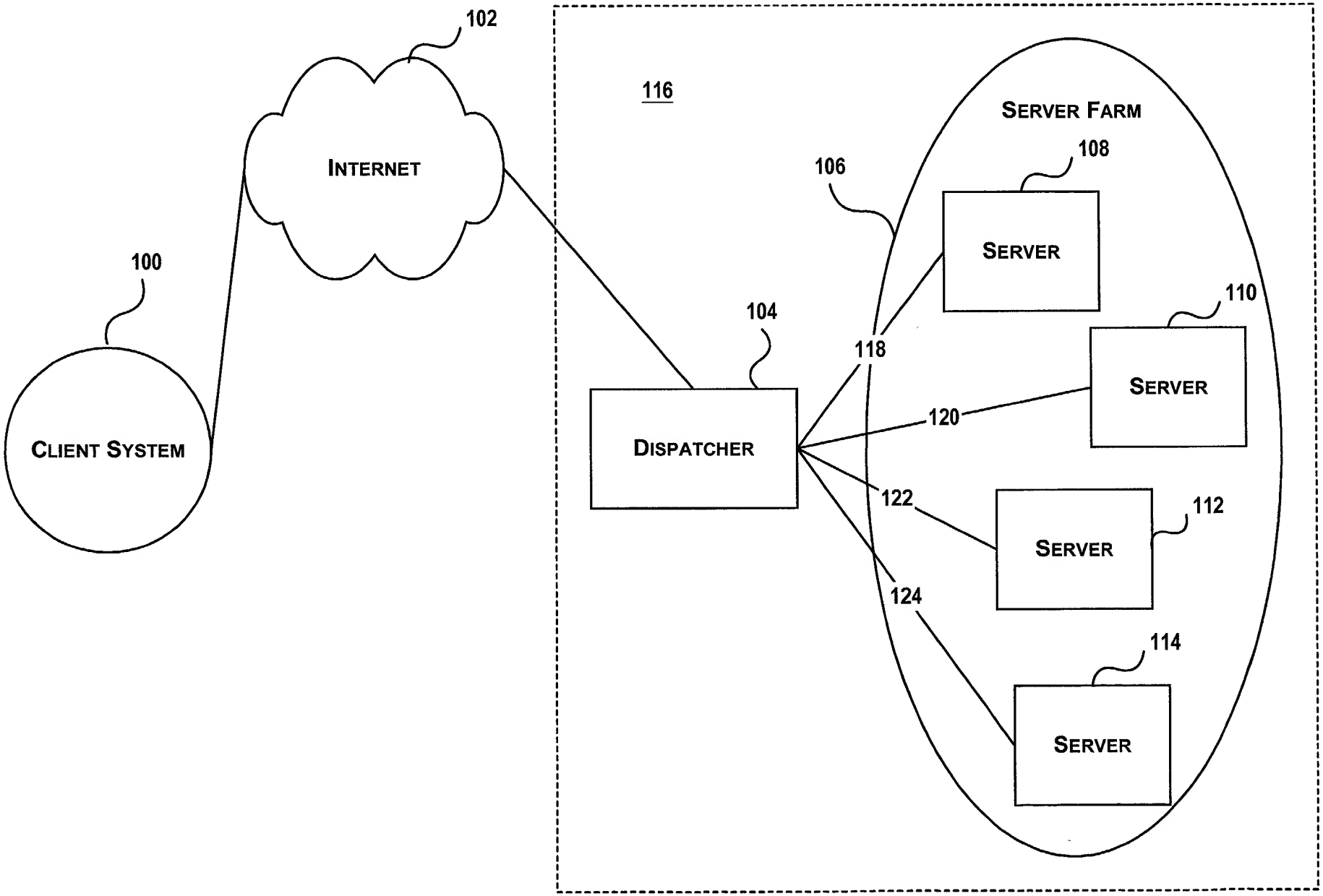

FIG. 1

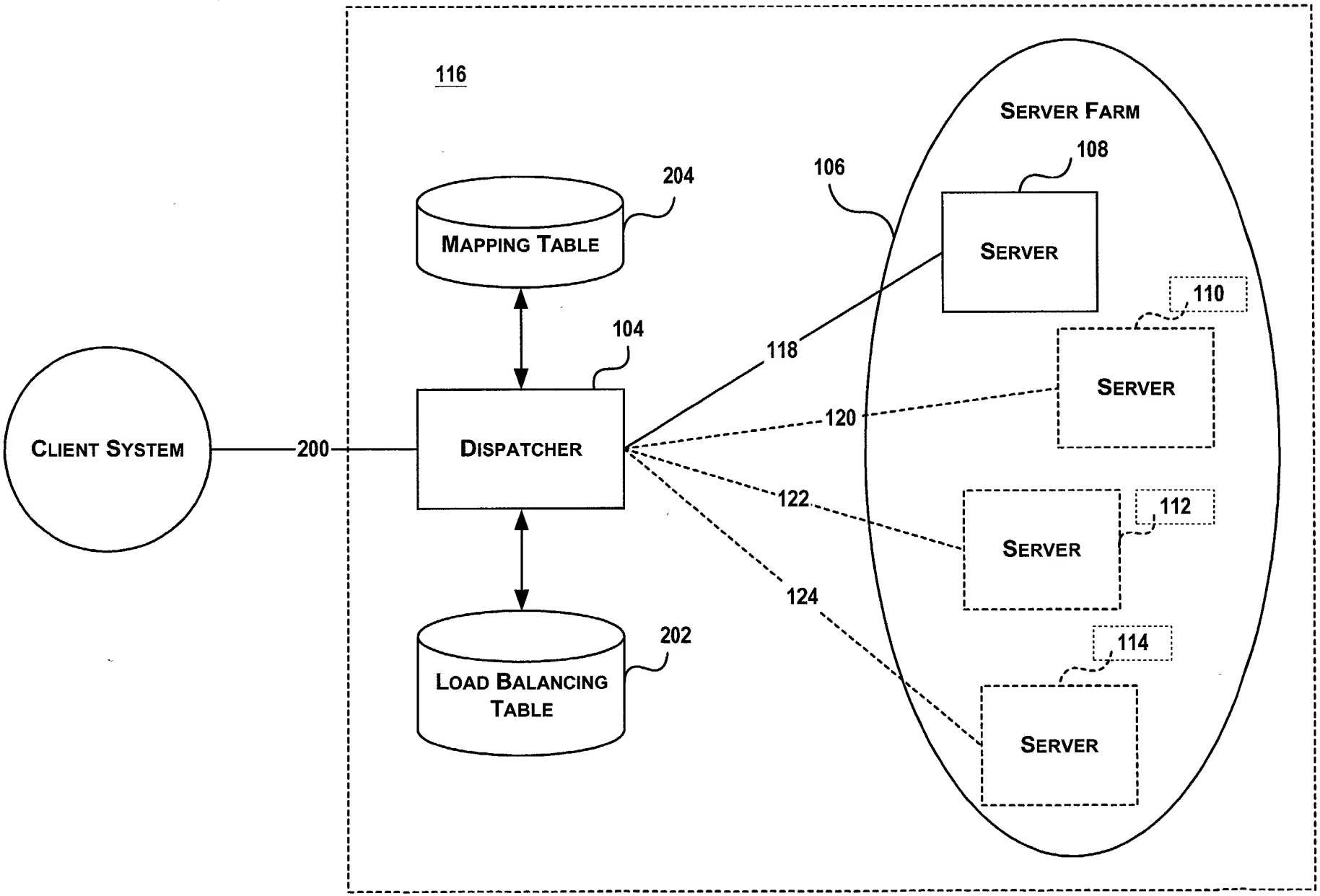
116
SERVER FARM
108
106
204
MAPPING TABLE
SERVER
110
104
118
SERVER
CLIENT SYSTEM
200
DISPATCHER
120
122
SERVER
112
124
114
202
LOAD BALANCING TABLE
SERVER

FIG. 2

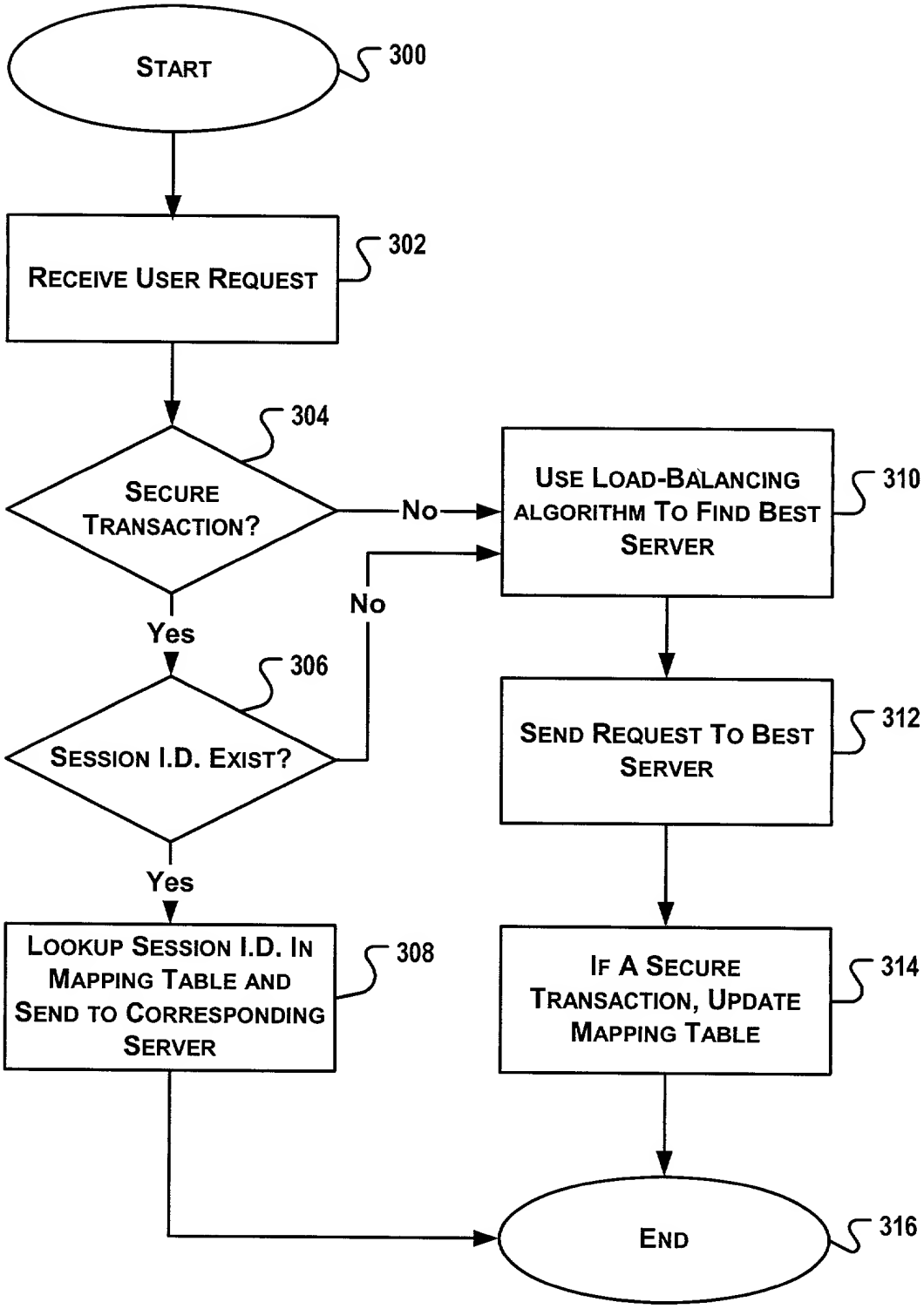
START
300
RECEIVE USER REQUEST
302
304
SECURE TRANSACTION?
No
USE LOAD-BALANCING ALGORITHM TO FIND BEST SERVER
310
Yes
No
306
SESSION I.D. EXIST?
SEND REQUEST TO BEST SERVER
312
Yes
LOOKUP SESSION I.D. IN MAPPING TABLE AND SEND TO CORRESPONDING SERVER
308
IF A SECURE TRANSACTION, UPDATE MAPPING TABLE
314
END
316

FIG. 3

006260 "6952960

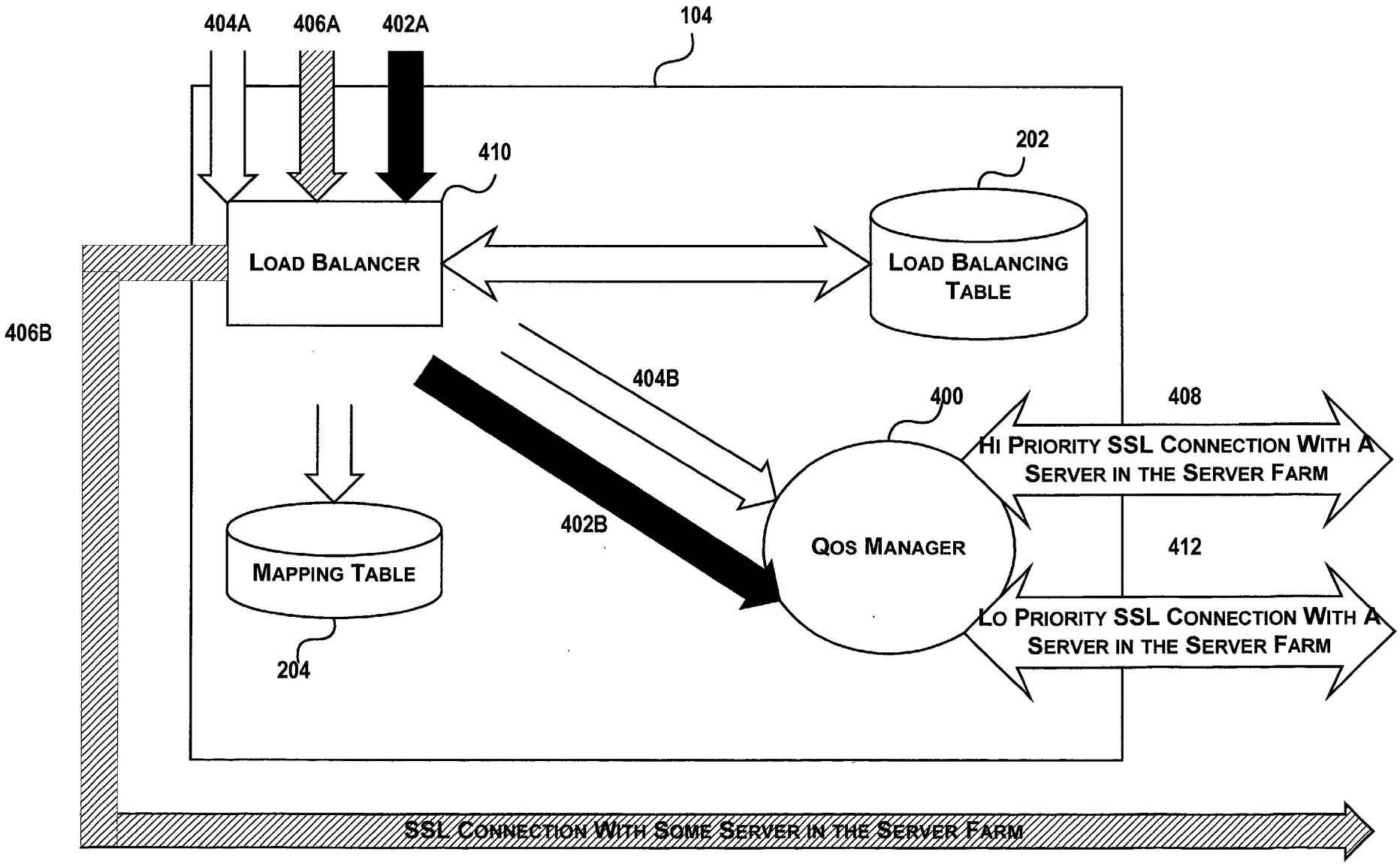

FIG. 4

Attorney's Docket No.: 042390.P9326 PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

MECHANISM FOR LOCKING CLIENT REQUESTS TO A PARTICULAR SERVER

the specification of which

_X_ is attached hereto.
___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

Application Number	Filing Date
Application Number	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Number	Filing Date	Status -- patented, pending, abandoned
Application Number	Filing Date	Status -- patented, pending, abandoned

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Libby N.Ho, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to (303) 740-1980.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Manav Mishra

Inventor's Signature _____ Date _____

Residence Hillsboro, OR (City, State) Citizenship United States of America (Country)

Post Office Address 2830 NW Overlook Drive #2225
Hillsboro, OR 97124

Full Name of Sole/First Inventor Satyendra Yadav

Inventor's Signature _____ Date _____

Residence Portland, OR (City, State) Citizenship Indian (Country)

Post Office Address 9523 NW Maring Drive
Portland, OR 97229

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. P44,587; Thomas M. Coester, Reg. No. 39,637; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Libby N.Ho, Reg. No. 46,774; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Erica W. Kuo, Reg. No. 42,775; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. P44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Kimberley G. Nobles, Reg. No. 38,255; Daniel E. Ovanezian, Reg. No. 41,236; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; James M. Wu, Reg. No. P45,241; Steven D. Yates, Reg. No. 42,242; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; Paramita Ghosh, Reg. No. 42,806; and Sang Hui Kim, Reg. No. 40,450; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. P44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.